The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
11/18/2020

SUBJECT:
A Vulnerability in Drupal Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in the Drupal core module, which could allow for remote code execution. Drupal is an open source content management system (CMS) written in PHP. Successful exploitation of this vulnerability could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:
- Drupal Core versions prior to 9.0.8, 8.9.9, 8.8.11, and 7.74

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in the Drupal core module, which could allow for remote code execution. The remote code execution vulnerability exists due to a lack of proper data sanitization of certain filenames on uploaded files. This can lead to files being interpreted as the incorrect extension, served as the wrong MIME type, or executed as PHP for certain hosting configurations.

Successful exploitation of this vulnerability could allow for remote code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Drupal to vulnerable systems immediately after appropriate testing.
- Ensure no unauthorized system changes have occurred before applying patches.
- Run all software as a non-privileged user to diminish effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services.
- Drupal version 8.7.x and earlier sites should be migrated to supported Drupal versions as soon as possible after patches are applied.

REFERENCES:
Drupal:
https://www.drupal.org/sa-core-2020-012

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13671